MCS Sp. z o.o.
Mazowieckie Centrum Stomatologii

ul. Nowy Zjazd 1
00-301 Warszawa
centrala: 22/ 55 69 300
sekretariat: 22/ 55 69 400
fax: 22/ 55 69 403

sekretariat@mcs-przychodnia.pl

MCS/ ZP/2211-477/2021

Warszawa, dn. 6 września 2021 r.

Do wszystkich uczestników postępowania
o udzielenie zamówienia publicznego

W nawiązaniu do zapytań dotyczących postępowania nr **ZZ/19/21 „Audyt bezpieczeństwa infrastruktury IT”,** informuję co następuje:

Pytanie nr 1.
Prosiłabym o odpowiedz na poniższe pytanie - dot. zmiany zakresu w niniejszym zapytaniu:
- Jak wygląda infrastruktura VPN do audytu? Ile punktów dostępu VPN znajduje się w zakresie audytu?
Ad1. jeden punkt dostępu

Pytanie nr 2.
- Ile baz danych jest przedmiotem audytu?
AD2. Dwie bazy danych

Pytanie nr 3.
- Co rozumieć przez „Audyt architektury bezpieczeństwa infrastruktury IT”? Czy mają Państwo jakiś konkretny standard według którego powinien być przeprowadzony audyt, czy mamy coś zaproponować?
Ad3. Proszę coś zaproponować

Pytanie nr 4.	**Odpowiedź**
Ile (szacunkowo) adresów IP znajduje się w sieci LAN (serwery, routery, firewalle, komputery, drukarki, laptopy, etc)?	ok. 150 aktywnych hostów (komputery, urządzenia sieciowe, etc)
Jaka jest lokalizacja sieci LAN? Jedna czy więcej?	
Czy testy maszyn znajdujących się w sieci wewnętrznej (LAN) muszą zostać wykonane w ramach prac on-site? Alternatywnie proponujemy podejście polegające na wykorzystaniu stacji przesiadkowej (komputer klasy Intel NUC), która instalowana jest w Państwa sieci. Dostęp zdalny do urządzenia realizowany jest poprzez zestawiany tunel VPN. Skany sieciowe wykonywane są ze wspominanego urządzenia, ale audytor nie musi pojawiać się w siedzibie Państwa firmy. Takie rozwiązanie ma wpływ na wycenę.	Nie dotyczy

Pytanie nr 5.	**Odpowiedź**
Ile publicznych adresów IP (lub jaka maska podsieci) będzie podlegać analizie?	4

Czy oferta ma zawierać retesty (tj. powtórne sprawdzenie czy wskazane w raporcie z testów podatności zostały skutecznie usunięte przez Zamawiającego)?	Tak

Pytanie nr6.	**Odpowiedź**
Do czego służy aplikacja?	rejestracja, anulownie wizyt,
Jak rozbudowana jest aplikacja (szacunkowa liczba unikalnych ekranów/formularzy, np. do 10, 50, 100, etc)?	do 50
Ile różnych grup użytkowników (o różnych uprawnieniach) posiada aplikacja i ile spośród nich musi zostać objętych audytem (rekomendujemy testy max. 3-4 grup)?	1
Ile endpointów/metod API wykorzystuje aplikacja (np. 10 endpointów/metod dla REST API, 10 operacji/metod w ramach 2 usług SOAP)?	Brak danych
W jakiej technologii wykonany jest system?	html5
W miarę możliwości proszę o przesłanie 2-3 zrzutów ekranowych z aplikacji.	
Jeśli audyt systemu ma obejmować audyt infrastruktury typu whitebox (analiza konfiguracji) proszę o podanie informacji jakie elementy miałyby zostać poddane testom – serwer HTTP (ile, jakie), baza danych (ile, jakie), system operacyjny (ile, jakie), np. (2 x Debian, 1 x PostgreSQL, 3 x Apache HTTPD)	1x SerwerHTTP ,2 x Oracle 11g, Centos, Oracle-linux
Czy możliwe są testy zdalne (np. z wykorzystaniem tunelu VPN)?	Tak
Na jakim środowisku będzie przeprowadzany audyt (testowe/produkcyjne)?	Produkcyjnym
Czy są jakieś ograniczenia czasowe w trybie przeprowadzania audytu (np. godziny nocne, etc.)?	Nie
Jaki jest pożądany termin wykonania audytu?	do końca 2021
Czy oferta ma zawierać retesty (tj. powtórne sprawdzenie czy wskazane w raporcie z testów podatności zostały skutecznie usunięte przez Zamawiającego)?	Tak
W jaki sposób zrealizowane jest uwierzytelnianie do aplikacji (standardowa para login i hasło, certyfikaty, tokeny 2FA, etc)?	Standardowa
Czy aplikacja wykorzystuje dodatkowe metody autoryzacji wrażliwych operacji (np. przy pomocy kodów SMS, tokenów sprzętowych, tokenów mobilnych, certyfikatów kwalifikowanych, etc)?	Nie
Czy istnieje możliwość uzyskania dostępu do aplikacji przed złożeniem oferty (np. do wersji demo)?	Tak
Pytanie nr 7.	**Odpowiedź**

Ile sieci WiFi miałoby podlegać testom?	Nie posiadamy sieci WI-FI
Jaka jest fizyczna lokalizacja sieci WiFi? Czy takich lokalizacji jest więcej niż jedna (np. różne miasta)?	
Czy oferta ma zawierać retesty (tj. powtórne sprawdzenie czy wskazane w raporcie z testów podatności zostały skutecznie usunięte przez Zamawiającego)?	Nie dotyczy

Pytanie nr 8.	**Odpowiedź**
Jaki rodzaj serwera VPN miałby podlegać testom (np.: IPSec, OpenVPN, WireGuard, Global Protect, inny)?	Ipsec, SSL VPN
Ile serwerów (adresów IP) będzie podlegać weryfikacji?	1
Czy prace mogą być realizowane w godzinach roboczych?	Tak
Prosimy o informacjęczy audyt powinien zostać zrealizowany w modelu blackbox czy whitebox? Blackbox zakłada brak dodatkowej wiedzy o usłudze poza adresem IP. Whitebox przewiduje możliwość przekazania Wykonawcy framentów konfiguracji (kopii plików konfiguracyjnych) lub dostępu do konsoli administracyjnej.	Whitebox

Pytanie nr 9.	**Odpowiedź**
Prosimy o podanie informacji jakie elementy miałyby zostać poddane analizie konfiguracji – serwer HTTP (ile, jakie), baza danych (ile, jakie), system operacyjny (ile, jakie), np. 2 x Debian, 1 x MySQL, 3 x nginx, etc.	serwer HTTP-centos x1 Oracle 11gx2 oracle -linux
Weryfikacja konfiguracji przeprowadzana jest poprzez udostępnienie audytorom określonych plików konfiguracyjnych oraz przy pomocy tzw. skryptów audytorskich. Są to autorskie narzędzia (skrypty Bash, pliki wsadowe), które wraz z krótką instrukcją Wykonawca dostarcza Zamawiającemu do wykonania na serwerach wchodzących w zakres testów. Audytorom przekazywane są wyniki działania skryptów. Skrypty nie są w żaden sposób obfuskowane. Prosimy o potwierdzenie, że takie podejście jest dla Państwa akceptowalne.	Tak

Pytanie nr 10.

1. **Pytania ogólne:**

   a) Czy istnieje możliwość zdalnego wykonania testów (przy pomocy VPN, bezpośrednio przez Internet lub za pomocą naszego urządzenia CQ-box, ustanawiającego bezpieczne połączenie z infrastrukturą Klienta)?

Tak jeśli Państwa urządzenie obsługuje Foriclenta

b) Jeśli testy mają być przeprowadzone na miejscu, gdzie zlokalizowana jest siedziba (miasto/kraj)?

Warszawa

c) Czy są jakieś ograniczenia dotyczące ram czasowych wykonywania testów (dni, godziny, strefa czasowa, np. pon - pt 8:00 – 16:00 CET)?

Jeśli testy nie obciążą łącza to nie ma ograniczeń a jeśli obciążą to po 16 lu po 20

d) Dodatkowe uwagi i wymagania (specyficzna forma raportu itp.):

Wskazanie niedociągnięć zaproponowanie rozwiazań

Prosimy o udzielenie informacji na pytania dotyczące wybranych rodzajów usług:

2. Jeżeli w zakresie audytu znajdują się testy bezpieczeństwa infrastruktury, prosimy o udzielenie odpowiedzi na poniższe pytania:

a) Liczba adresów IP/hostów mających podlegać testom wraz z podziałem na adresy wewnętrzne i zewnętrzne:

2

b) Liczba sieci VLAN, które mają podlegać testom:

2

c) Jakie środowisko ma zostać poddane testom (produkcyjne / testowe)?

Produkcyjne

3. Jeżeli w zakresie audytu znajduje się analiza konfiguracji infrastruktury, prosimy o udzielenie odpowiedzi na poniższe pytania:

a) Liczba i typy systemów, urządzeń sieciowych oraz silników baz danych, które mają podlegać audytowi wraz z ich wersjami (np. 3 x Windows Server 2012, 2 x Linux CentOS, 1 x CISCO ASA, 3 x Oracle 12g):

2x Oracle linu 11 g, 1x Centos

4. Jeśli w zakresie audytu znajduje się analiza architektury IT i procesów pod kątem bezpieczeństwa, prosimy o udzielenie odpowiedzi na poniższe pytania:

a) Liczba, typ dokumentów i łączna liczba stron dokumentacji podlegającej audytowi:

Nie dotyczy

b) Czy istnieje konieczność analizy rozwiązania pod kątem określonych regulacji i standardów (np. ISO 27001, Rekomendacja D, PCI DSS, itp.?)

Nie dotyczy

c) Czy audyt w zakresie procesów i bezpieczeństwa będzie dotyczył tylko obszaru IT?

Nie dotyczy

d) Liczba osób, które są odpowiedzialne za obszar IT i Bezpieczeństwa (potrzebne do określenia liczby spotkań)?

Nie dotyczy

e) Miejsce przeprowadzenia wywiadów:

Nie dotyczy

f) Czy w dokumentacji opisane jest wszystko z zakresu audytu – czy stosowane są nieudokumentowane praktyki?

Nie dotyczy